

ECS Configuration Change Request

Page 1 of 1 Page(s)

1. Originator Byron V. Peters	2. Log Date: 07/08/03	3. CCR #: 03-0474	4. Rev: —	5. Tel: 301/883-4077	6. Rm #: 2013	7. Dept. SE
8. CCR Title: Install and test F-Secure SSH 3.2.3						
9. Originator Signature/Date Byron V. Peters /s/ 07/08/03			10. Class II	11. Type: CCR	12. Need Date: 7/15/2003	
13. Office Manager Signature/Date Carolyn Whitaker /s/ 07/08/03			14. Category of Change: Initial ECS Baseline Doc.		15. Priority: (If "Emergency" fill in Block 27). Emergency	
16. Documentation/Drawings Impacted (<i>Review and submit checklist</i>): Will be delivered with PSR			17. Schedule Impact:		18. CI(s) Affected: MSS	
19. Release Affected by this Change: 6A		20. Date due to Customer:		21. Estimated Cost: None - Under 100K		
22. Source Reference: <input checked="" type="checkbox"/> NCR (attach) <input type="checkbox"/> Action Item <input type="checkbox"/> Tech Ref. <input type="checkbox"/> GSFC <input type="checkbox"/> Other: ECSed24411, ECSed33571, ECSed37486						
23. Problem: (use additional Sheets if necessary) SSHv1 has been replaced by SSHv2 and needs to be removed from each system as it is a potential security vulnerability. SSH 2.4 has recently been revealed to have a potential security hole that should be fixed and the SSH 3.2 replacement has other bug fixes and improvements that should be implemented.						
24. Proposed Solution: (use additional sheets if necessary) The IRIX 6.5 and Solaris 8 packages have been generated from F-secure provided files. Request that the testing first in the IDG cell, the functionality lab strings 2 and 3, and the PVC be handed sequentially and on one CCR as the Goddard DAAC needs this release as quickly as possible. Instructions attached.						
25. Alternate Solution: (use additional sheets if necessary) N/A						
26. Consequences if Change(s) are not approved: (use additional sheets if necessary) The new AES cipher will not be available hampering performance.						
27. Justification for Emergency (If Block 15 is "Emergency"): GDAAC needs the release ASAP in order to fully implement secure ingest.						
28. Site(s) Affected: <input checked="" type="checkbox"/> EDF <input checked="" type="checkbox"/> PVC <input type="checkbox"/> VATC <input type="checkbox"/> EDC <input type="checkbox"/> GSFC <input type="checkbox"/> LaRC <input type="checkbox"/> NSIDC <input type="checkbox"/> SMC <input type="checkbox"/> AK <input type="checkbox"/> JPL <input type="checkbox"/> EOC <input type="checkbox"/> IDG Test Cell <input type="checkbox"/> Other						
29. Board Comments:			30. Work Assigned To:		31. CCR Closed Date:	
32. EDF/SCDV CCB Chair (Sign/Date): Kevin Lange /s/ 07/09/03			Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS			
33. M&O CCB Chair (Sign/Date):			Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS			
34. ECS CCB Chair (Sign/Date):			Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ESDIS			

ADDITIONAL SHEET

CCR #: 03-0474 **Rev:** — **Originator:** B.V. Peters

Telephone: 301/883-4077 **Office:** 2103

Title of Change: Install and test F-Secure SSH 3.2.3

7. COTS Installation Instructions

7.1 Prerequisites

There are no prerequisites. Approximate installation time for average systems administrator per host: 15 minutes

Space required: 75MB for install 0-10MB in operations

No reboot is required.

7.2 Uninstall Instructions

On a Sun system, from root, execute the command:

```
# pkgrm fssh32
```

On an SGI system, from root, execute the command:

```
# versions remove fssh32
```

7.3 Installation Instructions

7.3.1 Sun installation

1. Login to host as root or su to root.
2. Copy the ssh32.tar.gz file to /tmp or other convenient location (net/admin?).
3. Change directory to that location. For example:
cd /tmp
4. Explode the file using the command:
gzip -dc ssh32.tar.gz | tar -xvf -
5. Change directory to the ssh32 install directory using the command:
cd ssh32
6. Explode the Sun tarfile using the command:
tar -xvf ssh32.sunpkg.tar
7. Backup the existing files using the command:
cpssh.sh

NOTE: By default, this puts all the files in /tmp/bssh and creates a tar file /tmp/<hostname>.bssh24.tar
ECS systems engineering recommends backing up the tar file to somewhere else in the event of a problem.

8. Verify that the system has the old versions of ssh using the command:

```
# pkginfo | grep ssh
```

If the response is positive, do step 9. Otherwise skip to step 10.

9. Remove the old packages using the command:

```
# pkgrm ssh21
```

(answer "y" to any questions asked)

```
...
```

```
# pkgrm ssh20
```

(answer "y" to any questions asked)

```
...
```

NOTE: If either package fails to be removed, note the error. If it is a file missing, copy the file from the backup you made in /tmp/bssh

10. Install the new TCP Wrappers package using the command:

```
# pkgadd -d /tmp/ssh32 tcpw76
```

(answer "y" to and questions asked)

```
...
```

11. Install the new ssh package:

```
# pkgadd -d /tmp/ssh32 fssh32 □
```

(answer "y" to any questions asked)

```
...
```

12. Edit /etc/ssh2/ssh2_config to uncomment the appropriate lines for SocksServer (not needed for EDF)

DefaultDomain

13. Edit /etc/ssh2/sshd2_config to uncomment the appropriate line for: AllowSHosts

14. After editing, restart the daemon using the command:

- ```
/etc/init.d/sshd2 restart
```
15. Remove the install directory as required.  

```
rm -rf /tmp/ssh32
```
  16. If desired, you may turn on log rotation using the commands:  

```
/usr/local/sbin/ssh.log_rot
/usr/local/sbin/wrap.log_rot
```
  17. Logoff from root and login as a normal user.
  18. Do some quick checks to verify that the install such as:  

```
% ps -ef | grep sshd2 (should show at least one process spawned recently by PID 1)
% ssh2 <differenthost>
% scp2 localtestfile remotehost:
```

19. Logoff.

### 7.3.2 SGI Installation

1. Login to host as root or su to root.
2. Copy the ssh32.tar file to /tmp or other convenient location (net/admin?).
3. Change directory to that location. For example:  

```
cd /tmp
```
4. Explode the file using the command:  

```
gzip -dc ssh32.tar.gz | tar -xvf -
```
5. Change directory to the ssh32 install directory using the command:  

```
cd ssh32
```
6. Explode the SGI tarfile using the command:  

```
tar -xvf ssh32+.sgiinst.tar
```
7. Backup the existing files using the command:  

```
cpssh.sh
```

NOTE: By default, this puts all the files in /tmp/bssh and creates a tar file /tmp/<hostname>.bssh24.tar

ECS Systems Engineering recommends backing up the tar file to somewhere else in the event of a problem.

8. Verify that the system has the old versions of ssh using the command:

```
versions | grep ssh
```

If the response is positive, do step 9. Otherwise skip to step 10.

9. Remove the old packages using the commands:

```
versions remove ssh21
versions remove ssh20
```

NOTE: If either package fails to be removed, note the error. If it is a file missing, copy the file from the backup you made in /tmp/bssh.

10. Change directory to the sgi install directory

```
cd sgi
```

NOTE: this should put you in /tmp/ssh32/sgi

11. Install the new package:

```
inst
inst> from
inst> .
inst> step
(make sure there are "i"s next to each of the fssh32 and tcpw76 modules)
inst> go
(answer yes to any questions asked. There should be no conflicts...)
inst> quit
```

12. Edit /etc/ssh2/ssh2\_config to uncomment the appropriate lines for SocksServer (not needed for EDF)  
DefaultDomain
13. Edit /etc/ssh2/sshd2\_config to uncomment the appropriate line for:  
AllowSHosts
14. If you had to change the AllowSHosts line, restart the server using the command:  

```
/etc/init.d/sshd2 restart
```
15. Remove the install directory as required.  

```
rm -rf /tmp/ssh32
```
16. If desired, you may turn on log rotation using the commands:  

```
/usr/local/sbin/ssh.log_rot
/usr/local/sbin/wrap.log_rot
```
17. Logoff as root and login as a normal user.
18. Do some quick checks to verify that the install such as:  

```
% ps -ef | grep sshd2 (should show at least one process spawned recently by PID 1)
% ssh2 <differenthost>
% scp2 localtestfile remotehost: □
```

19. Logoff